FORTUNE

The Coincheck Cryptocurrency Hack: Everything You Need to Know

By **REUTERS** January 29, 2018

Hackers have stolen roughly 58 billion yen ($532.60 million) from Tokyo-based cryptocurrency exchange Coincheck, raising questions about security and regulatory protection in the emerging market of digital assets.

The following are some questions and answers about one of the largest heists of cryptocurrencies in the history:

What Is NEM?

NEM is a cryptocurrency launched in March 2015 by a team of five developers identifying themselves as Pat, Makoto, Gimre, BloodyRookie and Jaguar. Its acronym stands for New Economy Movement and, like other cryptocurrencies, markets itself as a digital coin outside the control of governments and central banks, which can be used for fast, global transactions.

It is now the tenth largest cryptocurrency, with $9 billion worth of NEMs in circulation, trading at just below $1 per coin.

NEM was launched to rectify the high concentration of wealth that some in the cryptocurrency community believe to be one of the key weaknesses of bitcoin, the world's most widely known cryptocurrency, whose early adopters have turned into multi-billionaires.

Read: *Starbucks Chairman Schultz Rambles About Bitcoin on Earnings Call*

For bitcoin transactions to clear, computers compete to find the solution to a computational problem, which NEM developers say makes the rich richer as those who have money can afford more hardware to solve such problems.

NEM rewards accounts that participate in the economy. The balance of an account, who transacts with that account, and how much it transacts with others are all combined to calculate an account's importance, based on which transactions are cleared.

How Was Coincheck Hacked?

Many details are still unclear.

Yusuke Otsuka, Coincheck's chief operating officer, said on Friday that around 523 million NEM coins were sent from a NEM address at Coincheck at around 3 a.m. local time. Over eight hours later, Coincheck noticed an abnormal decrease in the balance.

Coincheck said the NEM coins were stored in a "hot wallet" instead of a "cold wallet." Company President Koichiro Wada cited technical difficulties and a shortage of staff.

What Is a Hot Wallet

Hot wallets are connected to the internet, therefore vulnerable to hacking. Experts warn that holding large sums in hot wallets is the equivalent of carrying large amounts of cash in person.

Cold wallets, such as Trezor and Ledger Nano S, are devices which can be as small as a USB stick and can be stored offline. Some keep them in a safe.

How Are Crypto Exchanges Regulated in Japan?

Japan's government in April recognized bitcoin as a legally accepted means of payment, and required exchange operators to register with the financial regulator.

The move — which came in the wake of the 2014 collapse of Tokyo-based Mt. Gox, then the world's largest bitcoin exchange — was designed to protect consumers and clamp down on illegal use of cryptocurrencies. It also formed part of Prime Minister Shinzo Abe's push to stimulate growth via the fintech sector.

The Financial Services Authority's requirements for would-be exchanges include robust computer systems and segregation of cash and cryptocurrency accounts, checks on traders' identities and risk management systems.

As of Jan. 17, the FSA had approved the registration of 16 Japanese cryptocurrency exchanges. A further 16 or so exchanges that were operating before the regulation was introduced — including Coincheck — have been allowed to continue operating on a provisional basis as their applications are assessed.

For more on cryptocurrency, watch Fortune's video:

Can Stolen NEMs Be Tracked?

The NEM.io Foundation, a Singapore-based organization supporting NEM blockchain technology, says it has a full account of the whereabouts of Coincheck's hacked NEM, tracing the currency on the blockchain shared ledger.

The hacker has not moved any of the funds, the foundation said in a statement posted to the Medium publishing site, adding it would create an automated tagging system within two days to follow the coins and identify any account which receives them.

It is unclear how the holders would be identified.

How Can Investors Avoid Being Hacked

Bitcoin evangelists recommend steering clear of centralized exchanges, arguing that the whole point of decentralized currencies was to not hand over control to third parties, such as central banks, commercial banks and exchanges, which raises the risk of mismanagement, scams or hacking.

Experts say only money needed for upcoming transactions should be kept in hot wallets. Even then, trading one cryptocurrency for another can be done over decentralized exchanges, such as Shapeshift, Changelly or Waves Dex, directly from the holder's wallet and not from a wallet controlled by an exchange in their name.

Risks of fraud or hacking then only occur when a holder wants to exchange crypto assets for fiat currencies, but these can be minimized. Transactions can be done peer-to-peer in a safe, public place amongst members of the local crypto community rated by reputation on websites such as localbitcoins.com or via a centralized exchange, with the risk of hacking limited to the amount of time spent online to perform the transaction.